UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WISCONSIN

ECOLAB Inc., and NALCO COMPANY LLC d/b/a Nalco Water, an Ecolab Company and/or Nalco Water, Plaintiffs, v. JESSICA GRAILER, Defendant.	Case No.: 3:23-cv-00102-wmc

MEMORANDUM IN SUPPORT OF MOTION TO DISMISS PLAINTIFFS' COMPUTER FRAUD AND ABUSE ACT CLAIM

TABLE OF CONTENTS

Page

SUMMARY OF THE ARGUMENT 1

ARGUMENT 1

I. The conclusory allegations in the Amended Complaint do not meet the pleading standard under *Iqbal/Twombly*. 1

II. Plaintiffs' Count III fails to state a claim for violation of the CFAA. 2

A. The CFAA requires unauthorized access, damage, and monetary loss. 2

B. The "without authorization" provision requires revocation of authorization in an employment situation. 3

C. Plaintiffs' do not allege facts sufficient to find that Grailer accessed their network "without authorization." 4

D. The CFAA standard to exceed authorized access requires accessing data that is beyond the normal authorizations provided. 7

E. Plaintiffs have not alleged with specificity facts sufficient to find that Grailer "exceed[ed] authorized access." 8

F. Plaintiffs fail to allege sufficient facts to demonstrate "damage" or "loss" of at least $5,000. 9

1. The CFAA requires an impairment to data, a program, or a system.... 9

2. The Amended Complaint does not allege the required "damage." 10

3. Plaintiffs have not adequately alleged "loss." 11

CONCLUSION 12

TABLE OF AUTHORITIES

Page

Cases

Ashcroft v. Iqbal,
556 U.S. 662 (2009) 1, 2

Bashaw v. Johnson,
No. 11-2693-JWL, 2012 WL 1623483 (D. Kan. May 9, 2012) 10, 11

Bell Atl. Corp. v. Twombly,
550 U.S. 544 (2007) 1, 6

Condux Int'l, Inc. v. Haugum,
No. CIV 08-4824 ADM/JSM, 2008 WL 5244818 (D. Minn. Dec. 15, 2008) 9

Daughtry v. Atlanta Crane & Automated Handling, Inc.,
No. 2:10-CV-1371-AKK, 2012 WL 13024455 (N.D. Ala. Jan. 12, 2012) 12

Del Monte Fresh Produce, N.A., Inc. v. Chiquita Brands Int'l Inc.,
616 F. Supp. 2d 805 (N.D. Ill. 2009) 10

Deutsch v. Hum. Res. Mgmt., Inc.,
Case No. 19-CV-5305 (VEC), 2020 WL 1877671 (S.D. N.Y. April 15, 2020) 5

Domain Name Comm'n Ltd. v. DomainTools, LLC,
449 F. Supp. 3d 1024 (W.D. Wash. 2020) 3

Facebook, Inc. v. Power Ventures, Inc.,
844 F.3d 1058 (9th Cir. 2016) 5

Farmers Ins. Exch. v. Auto Club Grp.,
823 F. Supp. 2d 847 (N.D. Ill. 2011) 9

Landmark Credit Union v. Doberstein,
746 F. Supp. 2d 990 (E.D. Wis. 2010) 9

LVRC Holdings LLC v. Brekka,
581 F.3d 1127 (9th Cir. 2009) 4, 7

New S. Equip. Mats, LLC v. Keener,
989 F. Supp. 2d 522 (S.D. Miss. 2013) 11

NW Monitoring LLC v. Hollander,
534 F. Supp. 3d 1329 (W.D. Wash. 2021) 5

Pable v. Chicago Transit Auth.,
No. 19-CV-7868, 2022 WL 2802320 (N.D. Ill. July 18, 2022) 7

QVC, Inc. v. Resultly, LLC,
159 F. Supp. 3d 576 (E.D. Pa. 2016) 3, 5

Riley v. Vilsack,

665 F. Supp. 2d 994 (W.D. Wis. 2009) 2

Schwartz v. ADP, Inc.,
No. 2:21-CV-283-SPC-MRM, 2021 WL 5760434 (M.D. Fla. Dec. 3, 2021) 12

TriTeq Lock & Sec. LLC v. Innovative Secured Sols., LLC,
No. 10 CV 1304, 2012 WL 394229 (N.D. Ill. Feb. 1, 2012) 12

United Fed'n of Churches, LLC v. Johnson,
522 F. Supp. 3d 842 (W.D. Wash. 2021) 4, 5

Van Buren v. United States,
141 S. Ct. 1648 (2021) 3, 7, 8

Viera v. Gen. Auto. Ins. Servs.,
No. 3:19-CV-00901, 2021 WL 396687 (M.D. Tenn. Feb. 4, 2021) 6

Statutes

18 U.S.C. § 1030 ..... 2, 7, 9, 11

Rules

Fed. R. Civ. P. 12(b)(6) 1

Legislative Materials

H.R. REP. NO. 98-894 (1984) 2

Other Authorities

C. Wright & A. Miller,
Federal Practice and Procedure (3d ed. 2004) 2

SUMMARY OF THE ARGUMENT

Plaintiffs' threadbare allegations regarding Grailer's alleged wrongdoing do not meet the *Iqbal/Twombly* pleading standards. Nowhere do Plaintiffs articulate with particularity facts that, if true, could support a violation of the Computer Fraud and Abuse Act (CFAA). Plaintiffs acknowledge, in fact, that Grailer, as an employee, was authorized to use Plaintiffs' network. The Amended Complaint contains no factual allegations supporting Plaintiffs' claim that Grailer accessed their network without authorization or that she exceeded her authorized access. Plaintiffs do not allege the date they purportedly terminated Grailer's employment (after she provided notice of her resignation), when they explicitly revoked her authorization to access the network, or whether and when they took steps to block her access. Nor, separately, do Plaintiffs sufficiently allege in their Amended Complaint facts to support any damage or loss. The CFAA requires factual support for its requisite "damage" and "loss" elements; Plaintiffs offer conclusory allegations that merely parrot the statutory language. Because Plaintiffs do not plead facts with sufficient specificity to maintain a claim and recover under the CFAA, Grailer respectfully requests that Plaintiffs' Count III be dismissed with prejudice.

ARGUMENT

I. The conclusory allegations in the Amended Complaint do not meet the pleading standard under *Iqbal/Twombly*.

Federal Rule of Civil Procedure 12(b)(6) requires a Court to dismiss a cause of action that fails to state a claim upon which relief can be granted. Fed. R. Civ. P. 12(b)(6). A blanket assertion of entitlement to relief is not sufficient. *See Ashcroft v. Iqbal*, 556 U.S. 662, 678–79 (2009); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 n.3 (2007). The Court likewise need not accept as true "threadbare recitals of a cause of action's elements, supported by mere conclusory statements." *Id.* 556 U.S. at 663. "*Twombly* and *Iqbal* establish two new principles of pleadings

in all cases: (1) 'fair notice' alone will not suffice; a complaint must be 'plausible' as well; and (2) a court may not accept 'conclusory' allegations as true." *Riley v. Vilsack*, 665 F. Supp. 2d 994, 1002 (W.D. Wis. 2009). Thus, "the pleading must contain something more... than... a statement of facts that merely creates a suspicion [of] a legally cognizable right of action." C. Wright & A. Miller, *Federal Practice and Procedure* § 1216, at 235–36 (3d ed. 2004). Where the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has not shown entitlement to relief. *Iqbal,* 556 U.S. at 678–79. The conclusory allegations in Count III of the Amended Complaint do not meet this standard.

II. Plaintiffs' Count III fails to state a claim for violation of the CFAA.

A. The CFAA requires unauthorized access, damage, and monetary loss.

The CFAA is primarily a criminal statute meant to "impose criminal sanctions upon 'hackers' and other criminals who access computers without authorization." H.R. REP. NO. 98-894, at 21 (1984). Congress carved out a civil remedy under 18 U.S.C. § 1030(g), which provides a remedy for those "who suffers damage or loss" in connection with a violation of the statute. Plaintiffs allege violations of two different provisions of § 1030(a) of the CFAA in Count III—§§ 1030(a)(2)(C) and 1030(a)(4). (*See* Dkt. 34, ¶¶ 93, 95). To establish civil liability under both sections, Plaintiffs must demonstrate that Grailer accessed a computer without authorization or exceeded her authorized access and that Plaintiffs, as a result, suffered damage or loss of at least $5,000. *See* 18 U.S.C. § 1030(c)(4)(A)(i)(I).

Here, Grailer's access to Plaintiffs' computer and/or network was authorized given her status as an employee. Plaintiffs do not sufficiently allege that Grailer's access was unauthorized or exceeded her authorized access. Separately, Plaintiffs have not identified any equipment or data damage, Plaintiffs have not alleged facts sufficient to support the claim that they suffered damage or loss of at least $5,000.

B. The "without authorization" provision requires revocation of authorization in an employment situation.

The Supreme Court recently addressed the scope and interpretation of the CFAA's phrases "without authorization" and "exceeds authorized access." *Van Buren v. United States*, 141 S. Ct. 1648 (2021). The "without authorization" clause protects computers from "outside hackers—those who 'acces[s] a computer without any permission at all." The "exceeds authorized access" clause protects computers from "inside hackers—those who access a computer with permission, but then 'exceed' the parameters of authorized access by entering an area of the computer to which [that] authorization does not extend." *Id.* at 1658. "[L]liability under both clauses stems from a gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system." *Id.* at 1658–59.

In the employment context, "those who have permission to access a computer for any purpose, such as employees, cannot act 'without authorization' unless and until their authorization to access the computer is specifically rescinded or revoked." *QVC, Inc. v. Resultly, LLC*, 159 F. Supp. 3d 576, 595 (E.D. Pa. 2016). For example, in *Domain Name Comm'n Ltd. v. DomainTools, LLC*, 449 F. Supp. 3d 1024, 1026–27 (W.D. Wash. 2020), on November 2, 2017, after the plaintiff detected that the defendant had violated the terms of use by collecting data in a prohibited manner from the plaintiff's server, the plaintiff sent the defendant a cease-and-desist letter. The plaintiff did not expressly revoke the defendant's right to access the servers until months later, on June 6, 2018. *Id.* at 1027. The plaintiff brought a claim under the CFAA alleging that the defendant's post-June 6, 2018, access was "without authorization." *Id.* In considering the issue of authorization, the court noted that "whether access is authorized or unauthorized 'depends on actions taken by the employer.'" *Id.* (quoting *LVRC Holdings LLC v.*

Brekka, 581 F.3d 1127, 1134–35 (9th Cir. 2009). "If the computer owner has not affirmatively rescinded the defendant's right to access the computer, any existing authorization/permission remains." *Id.* Given that the plaintiff did not affirmatively revoke the defendant's authorization to access the server until June 6, 2018, the defendant was deemed to have permission to access the servers before that date. *Id.* at 1027–28.

In short, if an employer gives an employee access to a computer network in connection with employment, the employer must formally revoke that authorization to maintain a claim under the CFAA, and in bring such a claim must allege when it formally revoked the given authorization. It is not sufficient to merely allege in conclusory fashion that an employee's access was not authorized. *See e.g., United Fed'n of Churches, LLC v. Johnson*, 522 F. Supp. 3d 842, 849 (W.D. Wash. 2021), *reconsideration denied*, No. C20-0509RAJ, 2022 WL 1093025 (W.D. Wash. Apr. 12, 2022) (dismissing CFAA claim because the allegations in the complaint did "not state when the revocation [of authorization] occurred, how that revocation was communicated, and what actions Defendants undertook afterwards.").

C. Plaintiffs' do not allege facts sufficient to find that Grailer accessed their network "without authorization."

Plaintiffs do not adequately plead that Grailer's alleged access was "without authorization." Taking Plaintiffs' allegations as true, while employed as Plaintiffs' Account Manager, Grailer was authorized to access Plaintiffs' network. (*See* Dkt. 34, ¶ 24 ("to perform her duties, Defendant was privy and given access to certain Company Trade Secret and Confidential Information.")). Plaintiffs do not allege *when* they rescinded or revoked Grailer's authorization to access their network. Because Plaintiffs do not allege specifically when Grailer's access to their computer and/or network became unauthorized or what she accessed that was off limits to her while she had authorization (i.e., when the gates were up or down with respect to

authorization, and whether the gates were up or down with respect to certain information), the facts alleged in the Amended Complaint do not state a claim under the CFAA. *See e.g., United Fed'n of Churches*, 522 F. Supp. 3d at 849; *QVC, Inc.*, 159 F. Supp. 3d at 595.[1] At most, the Amended Complaint contains either ambiguous statements allegedly made to Grailer about her responsibilities as an employee after she informed her supervisor that she was resigning, or conclusory allegations that Grailer was not authorized, without any supporting evidence.[2] *See Deutsch v. Hum. Res. Mgmt., Inc.*, Case No. 19-CV-5305 (VEC), 2020 WL 1877671, at *2 (S.D.N.Y. April 15, 2020) ("The court is not required, however, to credit mere conclusory statements[.]") (internal quotations omitted).

Regarding Grailer's formal termination, the Amended Complaint is significant for what it does not say. The Amended Complaint does **not** contain allegations that Plaintiffs informed Grailer—verbally or in writing—that she could no longer access documents, files, or email from her work computer, work phones, or personal phone at any point during her "two weeks' notice" period (i.e., after her resignation and before she was terminated). Nor does the Amended Complaint contain allegations that Plaintiffs deactivated or restricted Grailer's account access after she resigned, which they had the capability to do and could have done at any point after

[1] *See also Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1066 (9th Cir. 2016) (one authorized to access a computer subsequently accesses the computer "without authorization" only "when the employer has rescinded permission to access the computer and the defendant uses the computer anyway") (citations omitted). Indeed, none of the allegations in the Amended Complaint describe an unequivocal or express revocation or rescission of Grailer's authority to access Plaintiffs' network. *See NW Monitoring LLC v. Hollander*, 534 F. Supp. 3d 1329, 1339–40 (W.D. Wash. 2021) ("[T]he law requires *express* revocation of previously granted authorization.") (emphasis in original).

[2] *See e.g.,* Dkt. 34, ¶ 2 ("after being instructed that she was no longer to do any work further for Plaintiffs"), ¶ 34 ("Defendant's supervisor advised her that she was done and relieved of all duties"), ¶ 39 ("after informing Plaintiffs of her resignation and after being told by Plaintiff to cease performing any and all work"), ¶ 96 ("after expressly being instructed that she was no longer authorized to access the Company's computer devices or computer network").

receiving her resignation. The Amended Complaint is silent as to when Plaintiffs terminated Grailer's access to their network.

Nor is there any basis here to support an implicit revocation of authority. In some instances, courts have found that an employer implicitly revoked network access on the date the employee is terminated. *See Viera v. Gen. Auto. Ins. Servs.*, No. 3:19-CV-00901, 2021 WL 396687, at *19 (M.D. Tenn. Feb. 4, 2021). Plaintiffs, however, do not allege when Grailer's employment was officially terminated. Instead, Plaintiffs obfuscate the timeline and Grailer's status as an employee without alleging a specific termination date.[3] The only instance in the Amended Complaint where Plaintiffs allege that Grailer accessed documents and files "after her termination" is in paragraph 38; however, this paragraph is devoid of any date that would indicate when that termination occurred. Moreover, the paragraphs that follow (i.e., ¶¶ 39–45) reference activity that allegedly occurred on January 8, 2023—a date on which Plaintiffs admit Grailer was employed. (*See* Dkt. 34, ¶ 50 ("Defendant continued to work for the Company through January 11, 2023.")). Even were these phrases sufficient to demonstrate that Grailer's access was implicitly revoked when she was terminated, they do not provide a date certain when that termination occurred. As such, Plaintiffs did not provide Grailer with fair notice or sufficient factual allegations "enough to raise a right to relief above the speculative level." *Twombly*, 550 U.S. at 555.

[3] *See e.g.,* Dkt. 34, ¶ 2 ("after being instructed that she was no longer to do any work further for Plaintiffs"), ¶ 34 ("Defendant's supervisor advised her that she was done and relieved of all duties"), ¶ 36 ("after Defendant Grailer was separated from employment"), ¶ 39 ("after informing Plaintiffs of her resignation and after being told by Plaintiff to cease performing any and all work"), and ¶ 47 ("several days after Plaintiff's [*sic*] separation from employment").

Plaintiffs have not pleaded facts sufficient to demonstrate when they implicitly or explicitly revoked Grailer's authorization to access their network. *See LVRC Holdings LLC*, 581 F.3d at 1133–34 ("[A] person uses a computer 'without authorization'...when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway."). As such, Plaintiffs have not properly alleged that Grailer's access to their network was "without authorization."

D. The CFAA standard to exceed authorized access requires accessing data that is beyond the normal authorizations provided.

According to 18 U.S.C. § 1030(e)(6), "exceeds authorized access" means "access[ing] a computer with authorization and to use such access to obtain ... information in the computer that the accesser is not entitled so to obtain." In *Van Buren,* the Supreme Court resolved a Circuit split regarding the interpretation of this definition. 141 S. Ct. at 1654. The Court held that "an individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him." *Van Buren*, 141 S. Ct. at 1662. The Supreme Court's ruling was unambiguous: improper purpose or intent in accessing the information is insufficient to bring an "exceeds authorized access" claim under the CFAA. The information obtained via computer must constitute information for which the user has not been granted access. *Id.* Applying similar logic, the Northern District of Illinois held that a claim that an individual who was authorized to access the system, but then once inside took prohibited actions is "precisely the type of claim" held to be "outside the CFAA's scope." *Pable v. Chicago Transit Auth.*, No. 19-CV-7868, 2022 WL 2802320, at *1–2 (N.D. Ill. July 18, 2022).

E. Plaintiffs have not alleged with specificity facts sufficient to find that Grailer "exceed[ed] authorized access."

The Amended Complaint does not allege sufficient or specific facts to support Plaintiffs' claim that Grailer "exceed[ed] authorized access" to their network. Plaintiffs' Amended Complaint lacks any allegations that Grailer accessed files, folders, or databases that she had not been granted access to as part of her employment as an Account Manager for Plaintiffs. Plaintiffs offer conclusory allegations that Grailer "illegally" or "unlawfully" accessed Plaintiffs' trade secret and confidential information. (Dkt. 34, ¶¶ 45, 47). But at no point do Plaintiffs assert that their alleged trade secret and confidential information was not readily available to Grailer while she was employed as an Account Manager. In fact, they admit the opposite. (*See* Dkt. 34, ¶ 24 ("to perform her duties, Defendant was privy and given access to certain Company Trade Secret and Confidential Information.")).

Thus, according to *Van Buren's* gates-up-or-down inquiry, because Grailer had access to the trade secret information as part of her employment, there is no basis for a CFAA claim. *See Van Buren*, 141 S. Ct. at 1662 (finding defendant "did not 'excee[d] authorized access' to the database, as the CFAA defines that phrase, even though he obtained information from the database for an improper purpose" because there was no dispute that he had access to that information as part of his employment). Plaintiffs accordingly have not alleged facts sufficient to support a claim that Grailer's actions "exceed[ed] authorized access."

Plaintiffs have not alleged sufficient facts to support their claim that Grailer either accessed their network "without authorization" or that she "exceed[ed] authorized access." For this reason alone, Plaintiffs' claim under the CFAA should be dismissed.

F. Plaintiffs fail to allege sufficient facts to demonstrate "damage" or "loss" of at least $5,000.

Plaintiffs' CFAA claim separately fails because the Amended Complaint does not provide a factual basis for damage or loss in excess of $5,000 beyond conclusory and speculative statements.

1. The CFAA requires an impairment to data, a program, or a system.

Under the CFAA, the term "damage" means "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Courts have consistently held that "damage" refers to "the destruction, corruption, or deletion of electronic files, the physical destruction of a hard drive, or any diminution in the completeness or usability of the data on a computer system." *Farmers Ins. Exch. v. Auto Club Grp.*, 823 F. Supp. 2d 847, 852 (N.D. Ill. 2011) (internal quotations omitted). In analyzing the CFAA's damage requirement, courts have relied on the definition of "integrity" ("wholeness" or "soundness") to conclude that the CFAA's definition of damage requires "some diminution in the completeness or useability of data or information on a computer system." *Condux Int'l, Inc. v. Haugum*, No. CIV 08-4824 ADM/JSM, 2008 WL 5244818, at *7 (D. Minn. Dec. 15, 2008). "[T]he mere copying of electronic information from a computer system is not enough to satisfy the CFAA's damage requirement." *Farmers,* 823 F. Supp. 2d at 852. In fact, "seemingly every court in this circuit that has interpreted the meaning of the word 'damage' in the CFAA has held that damage does not encompass harm from the mere disclosure of information and the CFAA 'is not intended to expansively apply to all cases where a trade secret has been misappropriated by use of a computer.'" *Landmark Credit Union v. Doberstein,* 746 F. Supp. 2d 990, 993–94 (E.D. Wis. 2010).

To satisfy the "damage" element, a plaintiff must offer more than vague, conclusory allegations of damage and must provide facts to plausibly support damage. *Bashaw v. Johnson*, No. 11-2693-JWL, 2012 WL 1623483, at *1–3 (D. Kan. May 9, 2012). Conclusory allegations that a claimant "has been damaged," unaccompanied by allegations as to the nature of such damage, are insufficient to state a CFAA claim. *Id.* As the Northern District of Illinois explained, "copying electronic files from a computer database—even when the ex-employee e-mails those files to a competitor—is not enough to satisfy the damage requirement of the CFAA; there must be destruction or impairment to the integrity of the underlying data." *Del Monte Fresh Produce, N.A., Inc. v. Chiquita Brands Int'l Inc.*, 616 F. Supp. 2d 805, 811 (N.D. Ill. 2009), *on reconsideration in part* (May 13, 2009).

2. The Amended Complaint does not allege the required "damage."

Plaintiffs' CFAA claim fails as a matter of law because the allegations do not satisfy the "damage" requirement. There is nothing in the Amended Complaint suggesting that Plaintiffs have at any point lost access to the information they contend Grailer misappropriated. There are no allegations that email or other data servers were damaged, or that the equipment Grailer returned was damaged. Plaintiffs instead reference Grailer's actions as causing Plaintiffs "to suffer loss and damage to the integrity of data, computer systems and loss of confidential information and trade secrets." (Dkt. 34, ¶ 97). Plaintiffs cannot state a claim or satisfy the CFAA's damages requirement by offering conclusory allegations and parroting the statutory language. *See Bashaw*, 2012 WL 1623483, at *1–3. Likewise, Plaintiffs' allegations in the Amended Complaint that Grailer "downloaded" or "exfiltrated" files (she did not) is thus insufficient to demonstrate damage under the CFAA. *See Del Monte*, 616 F. Supp. 2d at 811.

To the extent Plaintiffs claim Grailer damaged them by resetting one of her work phones, the Amended Complaint does not include allegations that identify what data (if any) was permanently lost or destroyed. *See Bashaw*, 2012 WL 1623483 at *2 (finding assertion that "data was erased" without identification of the data that was allegedly erased insufficient). Based on the allegations related to the forensic investigation, Plaintiffs appear to be in possession of all the documents that Grailer allegedly accessed during her employment, including after verbally resigning on January 8, 2023, and just prior to her termination on January 18, 2023. *See New S. Equip. Mats, LLC v. Keener*, 989 F. Supp. 2d 522, 530 (S.D. Miss. 2013)**Error! Bookmark not defined.** (dismissing CFAA claim where "there [was] nothing in the complaint's factual allegations to indicate that Keener did more than copy files and transmit information").

For these reasons, Plaintiffs have not alleged facts to support the "damage" element as required for Plaintiffs to bring a civil violation under the CFAA.

3. Plaintiffs have not adequately alleged "loss."

Plaintiffs' CFAA claim fails as a matter of law because the allegations to do not satisfy the "loss" element of the statute. The term "loss" means "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). "The majority of courts have construed "loss" to include only two types of injury—costs incurred (such as lost revenues) because the computer's service was interrupted and costs to investigate and respond to computer intrusion or damage." *Bashaw*, 2012 WL 1623483 at *3. The Northern District of Illinois has specifically considered this issue and made the distinction between the two types of loss statutorily defined in the CFAA, holding that "an interruption of service" is required to recover lost revenue. *TriTeq Lock & Sec. LLC v. Innovative*

Secured Sols., LLC, No. 10 CV 1304, 2012 WL 394229, at *7 (N.D. Ill. Feb. 1, 2012); *see also Daughtry v. Atlanta Crane & Automated Handling, Inc.*, No. 2:10-CV-1371-AKK, 2012 WL 13024455, at *8 (N.D. Ala. Jan. 12, 2012) ("The CFAA's definition of 'loss' does *not* include lost revenue from the possible misappropriation of 'stolen' information.").

Plaintiffs do not allege sufficient facts to demonstrate that they have suffered any other "loss" under the CFAA. The Amended Complaint does not allege any interruption of service. Plaintiffs refer to work that their forensic expert performed, but they do not identify the costs incurred as a result of the alleged CFAA violation or even calculate the amount spent investigating. Indeed, although Plaintiffs allege that unspecified losses are "far in excess of $5,000" (Dkt. 34 at 97), they provide no factual allegations sufficient to establish that they actually incurred losses in this (or any other) amount. *See Schwartz v. ADP, Inc.*, No. 2:21-CV-283-SPC-MRM, 2021 WL 5760434, at *2 (M.D. Fla. Dec. 3, 2021) ("With just conclusory allegations on the damages element, the claim must fail.").

Because Plaintiffs have not alleged facts to demonstrate "damage" or "loss," Plaintiffs' CFAA claim should be dismissed.

CONCLUSION

For two independent reasons, Plaintiffs do not sufficiently allege a CFAA claim in their Amended Complaint. First, Plaintiffs do not allege facts sufficient to demonstrate that Grailer's access to Plaintiffs' network was "without authorization" or that she "exceed[ed] authorized access"—that is, Plaintiffs do not allege *when* they revoked authorization or *when* they officially terminated her employment. Second, Plaintiffs offer only vague and conclusory allegations of the damage and loss required to state a civil claim under the CFAA. Plaintiffs' CFAA claim should be dismissed with prejudice.

Respectfully submitted this 29th day of March, 2023.

/s/ Johanna M. Wilbert
Johanna M. Wilbert (SBN 1060853)
Shauna D. Manion (SBN 1091704)
QUARLES & BRADY LLP
411 E Wisconsin Avenue
Milwaukee, WI 53202
Telephone: (414) 277-5000
johanna.wilbert@quarles.com
shauna.manion@quarles.com

Matthew Splitek (SBN 1045592)
QUARLES & BRADY LLP
33 E. Main Street, Suite 900
Madison, WI 53703
Telephone: (608) 251-5000
matthew.splitek@quarles.com

Michael W. Carwin *(admitted in the W.D. Wis.)*
QUARLES & BRADY LLP
300 N. LaSalle Street, Suite 4000
Chicago, IL 60654
Telephone: (312) 715-5000
michael.carwin@quarles.com

Attorneys for Defendant